

עסקים בעידן הפרטיות והסייבר

עו"ד תומר שוירמן, מחלקת סייבר, ש. הורוביץ ושות'
כנס המסים והעסקים 2019



2018 - רוביקון

למה?

- תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017
- הליך פיקוח רוחב של הרשות להגנת הפרטיות
- General Data Protection Regulation
- חוק הגנת הפרטיות, תשמ"א-1981
- תקנות קיימות
- הנחיות הרשות להגנת הפרטיות (רמו"ט, בשמה הקודם)
- פסיקת בתי המשפט

Dr. Kosinski:

- 2008 עד 2015
- נטייה פוליטית, דת, צבע עור, נטייה מינית, נטייה לאלכוהול, סיגריות, וכו'
- 10 - קולגה לעבודה
- 70 - חברים
- 150 - בן משפחה
- 300 - בן/בת זוג
- ... +300

Cambridge Analytica:

- אבולוציה : עצרת בחירות - נאומים ברדיו - תשדירי טלוויזיה - תשדירים בחלוקה גיאוגרפית - תשדירים לפי זמני שידור - פרסום אינטרנטי - "ללחוש באוזן" במקום **לנאום בכיכר**
- טענות לפניות ממוקדות לציבור הבוחרים לקראת הבחירות לנשיאות ארה"ב, בדגש על "קולות מתנדנדים"
- טענות לפרטים אודות עשרות מיליוני משתמשים, שנאספו מאתר פייסבוק.
- אשליית הפרטיות?
- גבולות השימוש במידע אישי
- אחריות תאגידית, שימוש במידע על ידי צד שלישי

עידן המידע

צרכנות = מידע = פרטיות

סייבר

התפתחות

- מידע = כסף
- כלים טכנולוגיים שפותחים עולם חדש
- ההבדל המהותי בין לקוח אנונימי, לבין לקוח מזוהה
- חוק מור 1965
- Big Data ויכולות הצלבת מידע
- הרשאות
- עולם האפליקציות

תמורות עיקריות

הגשת תובענות ייצוגיות בארץ ובחו"ל בתחומים חדשים:

- אירוע אבטחה
- פרצות אבטחה
- הפרת הזכות לפרטיות (למשל בהעברת מידע לצדדים שלישיים ללא הסכמה)
- מדיניות פרטיות "בעייתית"
- רגולציה חדשה

רכיבים עיקריים

• אבטחה

• הסכמה

• שימוש

• העברה

• לסדר את המערכת

שימוש במידע – עקרונות בדין הישראלי

- רחב מאוד – כרוך בהסכמה
- עקרון צמידות המטרה
- פירוט והדגשה – דרישה הולכת ומתגברת

מהי הסכמה?

- מדיניות פרטיות – כמה ניתן להסתמך עליה?

אפשרות I:

אף אחד לא קורא את זה = חסר משמעות

אפשרות II:

לא קוראים כי בעצם מסכימים להכל ("Nothing to hide").

"Nothing to hide" – מהי הסכמה ?

"If you've got nothing to hide, you've got nothing to fear"

"Arguing that you don't care about **privacy**, because you have nothing to hide - is like arguing that you don't care about **free speech**, because you have nothing to say."

(Snowden)

אפשרות III:

תנאי מקפח בחוזה אחיד = עקרון העפרון הכחול.

הרשות להגנת הפרטיות

מה סמכותה?

עת"מ (ת"א) 24867-02-11 איי.די.איי חברה לביטוח בע"מ נ' רשם מאגרי המידע,

הרשות למשפט טכנולוגיה ומידע במשרד המשפטים (פורסם בנבו, 5.8.2012):

"הנה כי כן, הרשם פעל בגדר סמכותו עת הורה לעותרת לדווח הכיצד בכוונתה לפעול

למניעת פגיעה בפרטיות והפרת החוק בעתיד ועת הוציא הנחיה מפורשת לציבור

בעניין. עם זאת, ברור כי על ההחלטה או ההנחיה לעמוד במבחני הסבירות ולשקף

פרשנות ראויה וסבירה של הוראות החוק..."

תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017

- כניסה לתוקף - 8.5.2018.

- התקנות מסדירות את נושא אבטחת המידע, תוך פירוט משמעותי של הדרישות.

מהו "מידע"?

- "כלבי – לרבות חתול..."
- (מתוך חוקי עזר עירוניים שונים)
- חוק הגנת הפרטיות:
- "מידע" - נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו;
- "מידע רגיש" – נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו;
- חשוב – ככלל, אין "פרטיות" לתאגידים.

סיווג מאגרי המידע

- חלוקה לארבע קטגוריות, לפי רמת אבטחה נדרשת עולה:
 - מאגר המנוהל בידי יחיד;
 - מאגר החב ברמת אבטחה בסיסית;
 - מאגר החב ברמת אבטחה בינונית;
 - מאגר החב ברמת אבטחה גבוהה.

”שלב הזהב” - מיפוי מערכות המאגר

- יש להחזיק ולעדכן מסמך **מבנה מאגר המידע** ומערכותיו, אשר יכלול, בין היתר:
 - פירוט אודות תשתיות, לרבות מערכות חומרה, רכיבי תקשורת ואבטחת המידע.
 - מערכות תוכנה המשמשות להפעלה, ניהול, ניטור, תמיכה ואבטחת המאגר.
 - תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן.
- **תרשים הרשת** שפועל בה המאגר, כולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיסי.

דגשים ליישום:

- יותר תועלת מטרחה.
- חוצה ארגון – פח במכונית.
- מינוי אחראי.

נוהל אבטחת מידע

- יש לקבוע **נוהל אבטחת מידע** מפורט.
- הנוהל יכלול, בין היתר, התייחסות לנושאים הבאים:
 - האבטחה הפיסית של המאגר.
 - פירוט הרשאות הגישה למאגר.
 - תיאור אמצעי הגנת המאגר ואופן הפעלתם.
 - הסיכונים להם חשוף המאגר.
 - אופן ההתמודדות עם אירועי אבטחת מידע.
- יש לבחון את עדכון הנוהל לפחות אחת לשנה, וכאשר מתרחשים שינויים מהותיים במערכות המאגר או בסיכונים הטכנולוגיים להם הוא חשוף.

תיעוד ודיווח - אירועי אבטחת מידע

3. יישום הסמכות - אכיפה הדרגתית
 לאור ההערכות הנדרשת מבעלי, מנהלי ומחזיקי מאגרי מידע, החליטה הרשות לנקוט במדיניות אכיפה סובלנית כלפי המדווחים על אירוע אבטחה חמור בתקופת ההטמעה הראשונית ותקופת הביניים כמפורט להלן:

אכיפה במקרה של אי דיווח	אכיפה במקרה של ממצאים חריגים	אכיפה בעקבות דיווח	לוח זמנים	
קביעת הפרה ופרסומה (כולל פרסום אי הדיווח), התלייה או ביטול רישום המאגר	קביעת הפרה, במידת האפשר תוך הימנעות מפרסום	הנחייה לתיקון ליקויים	עד 31 בדצמבר 2018	תקופת הטמעה ראשונית
קביעת הפרה ופרסומה (כולל פרסום אי הדיווח), התלייה או ביטול רישום המאגר	קביעת הפרה	במקרים קלים – הנחייה לתיקון ליקויים, ביתר המקרים – קביעת הפרה	עד 30 ביוני 2019	תקופת הביניים
קביעת תוצר אכיפתי רגיל ע"פ מדיניות הרשות (כולל פרסום אי הדיווח), התלייה או ביטול רישום המאגר	קביעת תוצר אכיפתי רגיל ע"פ מדיניות הרשות	קביעת תוצר אכיפתי רגיל ע"פ מדיניות הרשות	החל מה- 1 ביולי 2019 ואילך	יישום מלא

מובהר כי כל המתואר לעיל מבטא מדיניות כללית בלבד, והרשות רשאית להקל או להחמיר במדיניות זו, בהתאם לנסיבות כל אירוע, מידת חומרתו, היקף הנזק והיקף נושאי המידע.

העברת מידע - מיקור חוץ

- מוקש.
- סוגים שונים של מיקור חוץ.
- תקנות הגנת הפרטיות (אבטחת מידע) (תקנה 15)
- **הנחית רשם מאגרי מידע מס' 2/2011 לעיבוד מידע אישי (outsourcing)**
שימוש בשירותי מיקור חוץ
קבלן מול מזמין
- יש לפקח על עמידת הקבלן בהסכם ובהוראות התקנות.

העברת מידע – מחוץ לגבולות ישראל

- תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001
- הסכמה / הסכמים / דין אירופאי

שירותי ענן

- האם שירותי הענן הם מיקור חוץ? האם חלות לגביהם החובות המנויות בתקנה 15 לתקנות אבטחת מידע?
- מתוך הנחיית רשם מאגרי המידע מס' 2/2011 בנושא שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי:
- "בכוונת הרשם לפרסם הנחיה אשר תעסוק בנושא השימוש בשירותי "מחשוב ענן" (cloud computing), שתהיה משלימה להנחיה זו."

שירותי ענן

- מתוך הדו"ח השנתי של רשם מאגרי מידע (רשות הגנת הפרטיות) לשנת 2015 :
- "מטרת המדיניות היא להגדיר את התהליך הנדרש לצורך קבלת החלטה של משרד ממשלתי אם להעביר או להקים מערכת מידע בענן ציבורי..."
- **הנורמות החלות במקרה זה** הינן תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001 והנחיית רשם מאגרי מידע 2-2011 שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי".

General Data Protection Regulation

- נושא אבטחת המידע, נכלל ב-GDPR ברמת ההנחיה הכללית.
- מנגד, ב-GDPR נכללות סוגיות רבות שממוקדות בנושא המידע וזכויותיו.
- רב הנסתר על הגלוי – ועוד יותר רב המלל...

GDPR – תחולה (Article 3)

• שאלת מיליון האירו

- ככלל, מי שמעבד (או אוסף) מידע אישי באיחוד האירופי לצורך הצעת טובין/שירות או מעקב אחר התנהגות.
- ככלל, פעילות הכרוכה בעיבוד של מידע אישי של אנשים באיחוד האירופאי.
- "This Regulation applies to the processing of personal data **in the context of the activities** of an establishment of a controller or a processor **in the Union**, regardless of whether the processing takes place in the Union or not."
- "This Regulation applies to the processing of personal data of **data subjects who are in the Union** by a controller or processor not established in the Union..."

GDPR – קנסות (Article 83)

- שאלת ה- "20 מיליון אירו"
- בגין הפרות מסוימות – קנסות בשיעור של עד 20 מיליון אירו או 4% מהמחזור הגלובלי השנתי, לפי הגבוה.
- Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to **20 000 000 EUR**, or in the case of an undertaking, up to **4 % of the total worldwide annual turnover** of the preceding financial year, whichever is higher...

GDPR – זכויות נושא המידע – הזכות לקבלת מידע (Article 15)

- נושא המידע זכאי לקבל פירוט נרחב אודות המידע הנאסף אודותיו, כולל קטגוריות המידע, זהות הגורמים החשופים למידע, מקורות המידע, פרופיילינג, וכו'.

- The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
 - the purposes of the processing;
 - the categories of personal data concerned;
 - the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations.

GDPR – זכויות נושא המידע – הזכות לקבלת מידע (Article 15)

- ...
- where the personal data are not collected from the data subject, any available information as to their source
- the existence of automated decision-making, including **profiling**...

הנחיית רשם מאגרי מידע בעניין דיוור ישיר

הנחיית רשם מאגרי מידע מס' 2/2017 - פרשנות ויישום הוראות חוק הגנת הפרטיות בעניין דיוור ישיר ושירותי דיוור ישיר (21.6.2017).

ספאם ודיוור ישיר

דגש על אופן משלוח דבר פרסומת – מול חיתוך ואפיון תת-קבוצה

• נקודות עיקריות :

- בחוזה אחיד, הדרך הרצויה לקבלת הסכמת הלקוח לשימוש במידע למטרת שירותי דיוור ישיר, שאיננה קשורה בתכלית העסקה, היא במתכונת של Opt In.
- Opt In = שתי תיבות לסימון : מסכים/לא מסכים
- פניה פרטנית – אינה דיוור ישיר (אך עלולה להיחשב כספאם).

הנחיית רשם מאגרי מידע בעניין דיוור ישיר

- "לעומת זאת, כשחברה (או תאגיד מסוג אחר) רוצה להפנות ללקוח שלה פניות בדיוור ישיר בעצמה, במיוחד אם הפניות מיועדות לשם הצעת שירותים או מוצרים בעלי זיקה לשירות העיקרי שמספקת החברה, **די לה שהחווה עם הלקוח יודיע ללקוח מראש על השימוש המתוכנן במידע אודותיו, ויאפשר ללקוח לסרב לשימוש במידע לצורך דיוור ישיר, אף אם המשמעות היא סירוב קבלת השירות בכללותו...**"

הנחיית רשם מאגרי מידע בעניין דיוור ישיר

- "עוד יש להדגיש, כי גם פניה של חברה (או תאגיד מסוג אחר) ללקוח שלה המבוססת על השתייכותו לקבוצת האוכלוסיה של לקוחותיה הפעילים, ואשר האפיון המשותף שלהם נובע רק מן המידע שמסרו בעצמם לחברה או מהמידע שהחברה אספה אודותם, לצורך מתן השירות לשמו התקשרו איתה הלקוחות - איננה מצויה בליבת פעולות עיבוד המידע אותן נועד סימן ב' להסדיר, משום שאיננה כרוכה ביצירת פרופיל אישיותי חדש על הלקוחות שלא היה נוצר ממילא לצורך מתן השירות, ומפני שהלקוחות מודעים ומסכימים לנסיבות יצירת הסיווג שלהם ולמקורותיו. לכן אין עניין להתייחס אליה כפניה "בדיוור ישיר" כהגדרתו בסעיף 17ג."

הנחיית רשם מאגרי מידע בעניין דיוור ישיר

- "לכן פניה של חברה לקוחותיה הפעילים, בלא שהחברה מבצעת לגביהם סיווגי משנה או יוצרת אודותם פרופילים חדשים שלא היו קיימים ממילא מעצם היותם לקוחות החברה – לא תתפרש כנכנסת לגדר "דיוור ישיר".
- וכך הדבר גם בנוגע לפניה לסוג מסויים של לקוחות פעילים שהמאפיין המשותף להם הוא גורם משמעותי ואינהרנטי בסוג השירות שמקבל הלקוח מהחברה; למשל: הגדרת לקוח בנק כ"חשבון חייל", "חשבון גמלאי" וכדו'."

הנחיית רשם מאגרי מידע בעניין דיוור ישיר

- "דרישה צורנית... ציון כי הפנייה היא בדיוור ישיר, בצירוף מספר הרישום של המאגר המשמש לשירותי דיוור ישיר כפי שהוא מופיע בפנקס מאגרי מידע. אם הפניה בדיוור ישיר איננה מבוססת על מידע שהגיע ממאגר לשירותי דיוור ישיר – אין חובה לציין את מספר רישום המאגר, אלא רק את זהות השולח והמקורות..."
- לעומת זאת, כאשר הנמען הוא לקוח פעיל של בעל המאגר הפונה אליו בדיוור ישיר – הלקוח מודע כמובן למקורות המידע (שהם מידע שמסר הלקוח עצמו במגעיו מול בעל המאגר) ולכן ככלל הרשם לא יאכוף את חובת היידוע."

תודה רבה!

כל הזכויות שמורות לש. הורביץ ושות' © 2018.
מצגת זו מיועדת למטרות אינפורמטיביות בלבד ואין בה משום התחייבות כלשהי לדיוק ו/או שלמות המידע הכלול בה. אין להתייחס ו/או להסתמך על הכתוב כעל ייעוץ משפטי מקצועי או תחליף לייעוץ שכזה. הסתמכות על תוכנה של מצגת זו ו/או שימוש בה, לא ייצרו בשום אופן יחסי עורך-דין – ללקוח בינך לבין ש. הורביץ ושות' ולא יהיה בהם כדי להטיל על ש. הורביץ ושות' אחריות כלשהי לתוצאות שתגרמנה מכך. תוכנה של מצגת זה והזכויות בה יישארו בכל עת בבעלות ש. הורביץ ושות'.

